



What is cryptocurrency and why do cybercriminals love it?

Posted: November 3, 2017 by [Wendy Zamora](#)

Last updated: November 2, 2017

Ever pretend you know what your friends are talking about because you want to sound smart and relevant—and then trap yourself in a lie?

“Wow, looks like those hackers were mining for cryptocurrency. You know what cryptocurrency is, right?”

“Oh yeah, totally. Cryptocurrency. Bad stuff. You know. Currency? In the crypt? Bad.”

“Yeah....”

Okay, so the *next* time someone asks, “What *is* cryptocurrency, anyway?” instead of awkwardly shrugging, be prepared to dazzle them with your insider knowledge.

What is cryptocurrency, in a nutshell?

In its simplest form, cryptocurrency is digital money. It’s currency that exists in the network only—it has no physical form. Cryptocurrency is not unlike regular currency in that it’s a commodity that allows you to pay for things online. But the way it was created and managed is revolutionary in the field of money. Unlike dollars or euros, cryptocurrency is not backed by the government or banks. There’s no central authority.

If that both excites and scares you, you’re not alone. But this technology train has left the station. Will it be a wreck? Or will it be the kind of disruptive tech that democratizes the exchange of currency for future generations?

If you take away all the techno-babble around cryptocurrency, you can reduce it down to a simple concept. Cryptocurrency is entries in a database that no one can change without fulfilling specific conditions. This may seem obtuse, but it's actually how you can define all currency. Think of your own bank account and the way transactions are managed—you can only authorize transfers, withdrawals, and deposits under specific conditions. When you do so, the database entries change.

The only major difference, then, between cryptocurrency and “regular” money is how those entries in the database are changed. At a bank, it's a central figure who does the changing: the bank itself. With cryptocurrency, the entries are managed by a network of computers belonging to no one entity. More on this later.

Outside of centralized vs. decentralized management, the differences between cryptocurrency and regular currency are minor. Unlike the dollar or the yen, cryptocurrency has one global rate—and worth *a lot*. As of November 2017, one Bitcoin is equal to \$6,942.77. Its value has increased exponentially this year, exploding from [around \\$800 in January 2017](#).

How does cryptocurrency work?

Cryptocurrency aims to be **decentralized**, **secure**, and **anonymous**. Here's how its technologies work together to try and make that happen.

Remember how we talked about cryptocurrency as entries in a database? That database is called the blockchain. Essentially, it's a digital ledger that uses encryption to control the creation of money and verify the transfer of funds. This allows for users to make **secure** payments and store money **anonymously**, without needing to go through a bank.

Information on the blockchain exists as a shared—and continuously reconciled—database. The blockchain database isn't stored in a single location, and its records are public and easily verified. **No centralized version** of this information exists for a cybercriminal to corrupt. Hosted by millions of computers simultaneously, its data is accessible to anyone on the Internet.

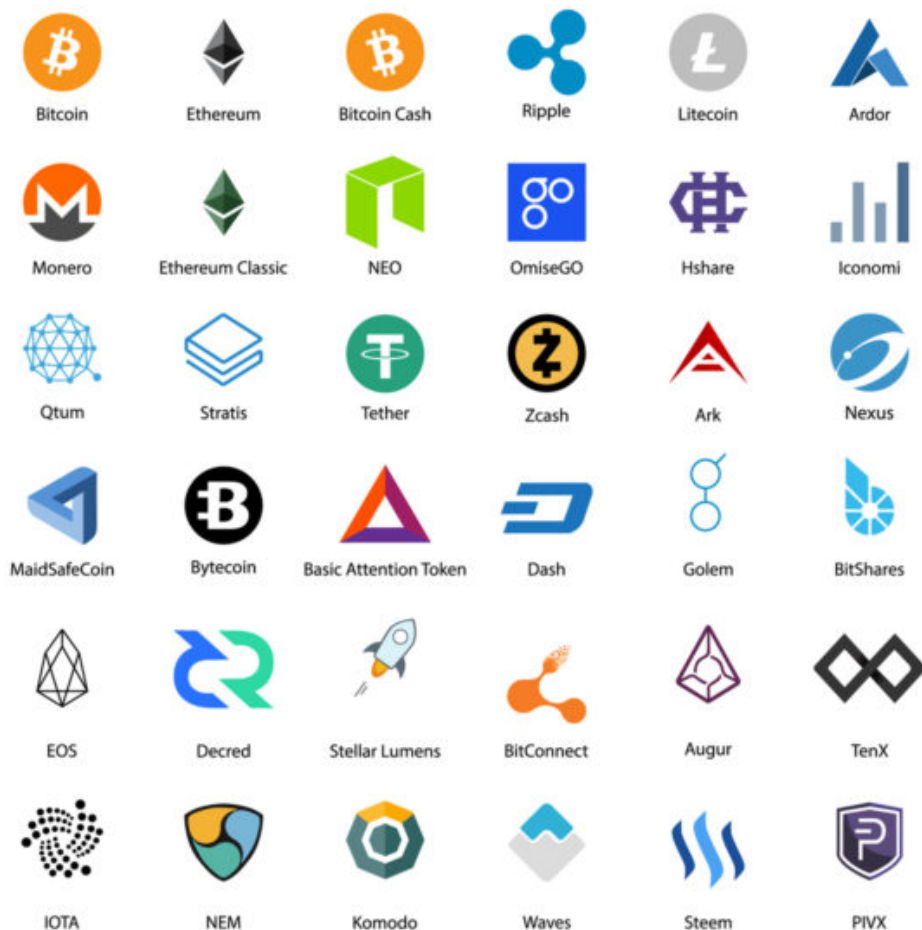
So how, exactly, is cryptocurrency created and maintained on the blockchain? Units are generated through a process called mining, which involves harnessing computer power (CPU) to solve complicated math problems. All cryptocurrencies are maintained by a community of miners who are members of the general public that have set up their machines to participate in validating and processing transactions.

And if you're wondering why a miner would choose to participate, the answer is simple: Manage the transactions, and earn some digital currency yourself. Those that don't want to mine can purchase cryptocurrency through a broker and store it in a cryptocurrency wallet.

When was cryptocurrency developed?

of eliminating the middle man in order to cancel interest fees, make transactions transparent, and fight corruption.

While Bitcoin was the first and remains the most popular cryptocurrency, others saw its potential and soon jumped on the bandwagon. [Litecoin](#) was developed in 2011, followed by [Ripple](#) in 2012. In 2015, [Ethereum](#) joined the fray and has become the second most-popular cryptocurrency. [According to CoinMarketCap](#), there are now more than 1,000 cryptocurrencies on the Internet.



Cryptocurrency's popularity on the Internet soon bled into other real-world applications. Japan has adopted Bitcoin as an official currency for commerce. Banks in India are using Ripple as an alternative system for transactions. [JP Morgan](#) is developing its own blockchain technology in partnership with Quorum, an enterprise version of Ethereum.

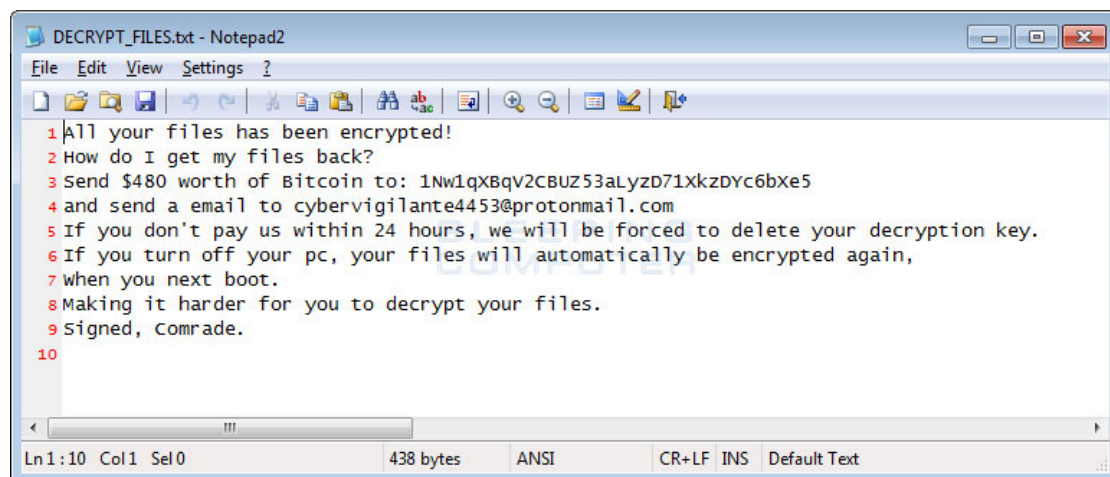
However, as with any new and relatively untested technology, the cybercriminals wanted in. And it wasn't long before Bitcoin and other cryptocurrencies fell victim to their own democratic ideals.

How has cryptocurrency been abused?

multitude of vulnerabilities. Like vultures to carrion, cybercriminals flocked to exploit. According to Hacked, [an estimated 10 to 20 percent](#) of all Bitcoin in existence is held by criminals.

While cryptocurrency was initially hailed as the next big thing in money, a savior for folks who just lost everything in steep recession (but watched as the banks that screwed them over walked away unscathed), a hack in 2011 showed how insecure and easily stolen cryptocurrency could be. Soon, the criminal-minded rushed in, looking to take advantage of the cheap, fast, permission-less, and anonymous nature of cryptocurrency exchange. Over the last nine years, millions of Bitcoin, worth billions of dollars, have been stolen—some events so major that they drove [people to suicide](#).

On a smaller but much more frequent scale, [cryptocurrency is used on the black market](#) to buy and sell credit card numbers and bot installs, fund hacktivism or other “extra-legal” activity, and launder money. It’s also the payment method of choice for ransomware authors, whose profits are made possible by collecting money that can’t be traced. Certainly makes getting caught that much more difficult.



Ransom note asking for Bitcoin

And if that weren't enough to call cryptocurrency unstable, the [process of mining itself is vulnerable](#) and has already attracted some high-profile hacks. [Services such as CoinHive](#) allow those that deploy it to mine the CPU of their site visitors—without the visitors' knowledge or permission. This process, known as [cryptojacking](#), is robbery-lite: Users may see an impact to their computer's performance or a slight increase in their electric bill, but are otherwise unaffected. Or that is, they were, until cybercriminals figured out how to [hack CoinHive](#).

Future applications

So where does that leave us with cryptocurrency? Surely its popularity is skyrocketing and its value is spiking so hard it could win a gold medal for beach volleyball at the Olympics. But is it a viable, safe alternative to our

We can see the technological applications for the future that demonstrate the clear advantages of cryptocurrency over our current system. But right now, cryptocurrency is good in theory, bad in practice. Volatile and highly hackable, we'll have to move to create security measures that can keep up with the development of the tech, otherwise cybercriminals will flood the market so heavily that it never moves beyond the dark web.

If you want to learn even more about cryptocurrency, stay tuned for a deeper dive on blockchain technology and a full report on cryptojacking.

SHARE THIS ARTICLE



COMMENTS

21 Comments **Malwarebytes Labs**

Login ▾

Recommend 6 Share

Sort by Best ▾



Join the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS

Name



RaptureSoon • 4 months ago

Thanks for sharing the enlightenment for many novices. The post was also shared on www.GAB.AI under the LIVE topic of Crypto <.!

7 ^ | v • Reply • Share ›



Wendy Zamora Mod ➔ RaptureSoon • 4 months ago

You're welcome! Thanks for sharing the post.

5 ^ | v • Reply • Share ›



George • 3 months ago

A very timely and informative item for those of us who might otherwise be tempted to get involved in something we don't quite understand.

2 ^ | v • Reply • Share ›

known (unknown by most people) as the Federal Reserve prints our paper money, that is not tied to any limiting resource like gold. It exists in as much or as little as the bankers decide! And besides the US money being printed and distributed to the Federal Government, at Interest, that (fiat) money can be recorded as some numbers on a ledger. Much like the checking accounts that we're familiar with, it's just an exchange of numbers. (It's the great numbers game, a party to which you and I are not invited.) I don't know much about Cryptocurrency, but I know that if I need organic food quickly, buying online is way too slow! And even if one saved a zillion dollars in this cryptocurrency, there are plenty of material things that I need that can't be had thru the internet. Moreover, there are non-material things, like Love, or Consciousness. But the main problem with our current system of currency in the US is that prices keep going up more than wages. I have to ask: Do you own a car, and can you afford to go on vacations? I remember over 50 years ago, when families took vacations, and most had 1 or 2 cars, if there were two drivers. Now...whom do YOU know who has any money to spare, other than just to pay bills? It's the bankers!!!

1 ^ | v • Reply • Share ›



Rich Quitlano • 3 months ago

Good article... I write on Steemit and get paid in Steem (one of the cryptos shown on your chart) It can easily be converted to fiat currency- in fact that's how I pay my Malwarebytes bill. By the way, as of this writing, BTC is over \$8000.

1 ^ | v • Reply • Share ›



Frank Hanson • 3 months ago

I must be missing something. If you need "Real Money" to buy "Digital Money" how is that revolutionary? It seems to be the same as buying a Stock.

^ | v • Reply • Share ›



Mike Griffin • 3 months ago

Thanks Think I wait and see where this goes? Investigate more.

^ | v • Reply • Share ›



Gary L. Smith • 3 months ago

Thanks for sharing! Great information and confirmation for me to NOT get involved, until the dust settles.

^ | v • Reply • Share ›



Ignatius Ibsage • 3 months ago

what happens if the internet goes down, e.g. a massive solar flare?

^ | v • Reply • Share ›



rick charles → Ignatius Ibsage • 3 months ago

Guess the non-existence money would vanish!?!?!?

Learned my lesson.



Wodie → rick charles • 3 months ago

Your "savings account" will also disappear, as it is just a collection of ones and zeros on some commercial bank's server. Hope you've got something tangible.

^ | v • Reply • Share ›



ScottyG → Wodie • a month ago

Wodie, you realize that banks and savings accounts were around before the internet? Right?

^ | v • Reply • Share ›



Gundamn → ScottyG • a month ago

and you realize they've moved all their data onto computers, right?

^ | v • Reply • Share ›



Marian Cates • 3 months ago

Thanks! Shared to fb and twitter.

^ | v • Reply • Share ›



Old_Fart • 3 months ago

What caused this irrational rise in the value of bitcoins? What affects its value?

^ | v • Reply • Share ›



tim_lester → Old_Fart • 3 months ago

How it is irrational when fiat can be created out of thin air? Value is subjective but most people mention that there is no middle man, no government manipulation(inflation, printing, bailouts, etc), low fees, transact anywhere in the world, etc. Does that sound valuable or do you think cash is more valuable where you have factors that you cannot control its store of value?

1 ^ | v • Reply • Share ›



Bob Deplorable Racist Smith → tim_lester • 3 months ago

One significant factor that you conveniently left out is that the "fiat" money is backed by the almighty tax payer dollar. Cryptocurrency...by nothing but pure supply/demand.

^ | v • Reply • Share ›



Old_Fart → tim_lester • 3 months ago

You did not answer my questions.

^ | v • Reply • Share ›



Bob Deplorable Racist Smith → Old_Fart • 3 months ago

Good old supply/demand. Plain and simple.



Vernon Hamilton • 5 months ago

A (relatively few) People with too much money, cant think of anything better to do with it besides bid up commodities. Bitcoin is going up so they jump in. The price of equity shares is also insanely over valued, simply because there is a lot of stupid money with no where to go.

^ | v • Reply • Share ›



Alain Bos • 4 months ago

Kinda f***ed are these coins. Now are there any "safe"-coins out there ? And what's up with this ransom-ware ? Is it just at particular sites or can this happen while surfing youtube too ? It does remind me to make a back-up more regularly than once a year.... Well Wendy, very good post, thanx for sharing ! and plz keep us updated !-)

^ | v • Reply • Share ›

RELATED ARTICLES

Stopping malware distribution at the source

May 9, 2012 - At Malwarebytes we are a bit obsessed with protecting our users, which causes us to approach our jobs from all sorts of different angles. One of my favorite aspects of this is how we tackle malware right at its source: the servers that deliver it. Our team works around the clock to identify and block...

[CONTINUE READING](#)

17 Comments

Telephony Scams: Can You Help?

May 24, 2012 - Back in 2009, I wrote about a telephony based scam that had gained momentum, and which sadly appears to have grown since then — invading other countries and scamming more victims. Since then, various other people, including my friends at Microsoft, have been investigating the companies involved, to try and both raise awareness and shut...

[CONTINUE READING](#)

2 Comments

Phishing 101: Part 1

[CONTINUE READING](#) 3 Comments

Phishing 101: Part 2

July 3, 2012 - “Over the years, phishing attacks have changed, as with most things, and have been segmented into different groups of variants.” –Me If there is one thing you can say about cybercriminals, it’s that they are adaptive. As I mentioned last week, phishing attacks have evolved from just fake web pages and official looking emails to...

[CONTINUE READING](#) 2 Comments

Phishing 101: Part 3

July 13, 2012 - Over the last few weeks I have described numerous methods of phishing attacks and a few examples what they do or may look like. In this final installment, I will shed some light on how phishing attacks are done and a few real world examples of techniques used by Phishing scammers. Finally, I will discuss...

[CONTINUE READING](#) 4 Comments

ABOUT THE AUTHOR

**Wendy Zamora** 

Head of Content, Malwarebytes Labs

Wordsmith. Card-carrying journalist. Lover of meatballs.

CATEGORIES

101

Malwarebytes news

PUP

Security world

SEARCH LABS



SUBSCRIBE

Email

GO

[Subscribe to RSS](#)

TOP POSTS

Tech support scammers find new way to jam Google Chrome (updated)

Panic attack: Apple scams apply pressure

Encryption 101: a malware analyst's primer

Drive-by cryptomining campaign targets millions of Android users

Kotlin-based malicious apps penetrate Google market

Cybersecurity info you can't do without

Want to stay informed on the latest news in cybersecurity? Sign up for our newsletter and learn how to protect your computer from threats.

SUBSCRIBE

HEADQUARTERS

Malwarebytes

3979 Freedom Circle, 12th Floor

Santa Clara, CA 95054

FOLLOW US



[EULA](#) [Privacy](#) [Terms of Service](#) © 2018 Malwarebytes

Language: English

